REMARKS

Claims 1-81 are pending in the Application. Claims 1-81 are rejected under 35 U.S.C. §112, second paragraph. Claims 1-81 are rejected under 35 U.S.C. §102(b). Applicant respectfully traverses these rejections for at least the reasons stated below and respectfully requests the Examiner to reconsider and withdraw these rejections.

Applicant notes that claim 8 was not amended to overcome prior art but to correct an insufficient antecedent basis problem. Hence, the amendment made to claim 8 was not narrowing in scope and therefore no prosecution history estoppel arises from the amendment to claim 8. *Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co.*, 62 U.S.P.Q.2d 1705, 1711-1712 (2002); 56 U.S.P.Q.2d 1865, 1870 (Fed. Cir. 2002). Further, the amendment made to claim 8 was not made for a substantial reason related to patentability and therefore no prosecution history estoppel arises from such an amendment. *See Festo Corp.*, 62 U.S.P.Q.2d 1705 at 1707 (2002); *Warner-Jenkinson Co. v. Hilton Davis Chemical Co.*, 41 U.S.P.Q.2d 1865, 1873 (1997).

I. REJECTIONS UNDER 35 U.S.C. §112:

The Examiner has rejected claims 1-81 under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. Paper No. 6, page 2. In particular, the Examiner states:

> Claims 1, 28, 55 essentially claim a method for bypassing a user sign-on screen by presenting the user with a sign-on screen. This language renders the claims vague and indefinite. For the purposes of examination, the claimed invention will be interpreted to be a method of bypassing a series of application sign-on screens by presenting the user with a single initial sign-on screen. Paper No. 6, page 2.

Applicant respectfully directs the Examiner's attention to the preamble of claim 1 which states "a method of bypassing an initial sign-on screen of an underlying operating system with a single sign-on capability." There is no language that states bypassing a user sign-on screen by presenting the user with a sign-on screen. Furthermore, Applicant respectfully contends that the scope of the claimed subject matter in claims 1-81 can be determined by one having ordinary skill in the art. The Examiner has not provided any evidence that a person of ordinary skill in the art would not be able to determine the scope of the claimed subject matter. A rejection under 35 U.S.C. §112, second paragraph, is not appropriate, when the scope of the claimed subject matter can be determined by one having ordinary skill in the art. M.P.E.P. § 706.03(d). As stated above, one having ordinary skill in the art can determine the scope of the claimed subject matter in claims 1-81. Consequently, Applicant respectfully asserts that claims 1-81 are allowable under 35 U.S.C. §112, second paragraph, and respectfully requests the Examiner to withdraw the rejections of claims 1-81 under 35 U.S.C. §112, second paragraph.

The Examiner further states:

> Claims 14, 21, 27, 41, 48, 54, 68, 75 and 81 recite the limitation of having a user log off and then re-logon in order to gain a different access level. This limitation appears to be in direct contrast to the apparent purpose of the invention which is to avoid having to logon multiple times per user. Paper No. 6, page 2.

Applicant respectfully directs the Examiner's attention to the language in claim 14 which states "wherein said switch user program logs off said user with said first level of access, wherein said underlying operating system logs on said user with said second level of access." The switch user program logs off the user with a first level of access and the underlying operating system logs on the user with the second level of access. There is no re-logging on by the user as asserted by the Examiner. Further, the purpose of the claim is not to explain technology or how it works. *S3 Inc. v. nVIDIA Corp.*, 59 U.S.P.Q.2d 1745, 1748 (Fed. Cir. 2001). The purpose is to state the legal boundaries of the patent grant. *Id.* Applicant respectfully asserts that the claimed subject matter in claims 14, 21, 27, 41, 48, 54, 68, 75 and 81 can be determined by one having ordinary skill in the art. The Examiner has not provided any evidence that a person of ordinary skill in the art would not be able to determine the scope of the claimed subject matter. A rejection under 35 U.S.C. §112, second paragraph, is not appropriate, when the scope of the claimed subject matter can be determined by one having ordinary skill in the art. M.P.E.P. § 706.03(d). As stated above, one having ordinary skill in the art can determine the scope of the claimed subject matter in claims 14, 21, 27, 41, 48, 54, 68, 75 and 81. Consequently, Applicant respectfully asserts that claims 14, 21, 27, 41, 48, 54, 68, 75 and 81 are allowable under 35 U.S.C. §112, second paragraph, and respectfully requests the Examiner to withdraw the rejections of claims 14, 21, 27, 41, 48, 54, 68, 75 and 81 under 35 U.S.C. §112, second paragraph.

The Examiner further states that the limitation of "said switch user program" in claims 8 and 9 lack antecedent basis. Paper No. 6, page 3. Applicant replaced the term "said" to be "a" in claim 8 prior to the phrase "switch user program" as indicated above thereby correcting the insufficient antecedent basis problem. Since claim 9 depends from claim 8, which recites "switch user program", the limitation of "said switch user program" in claim 9 does have sufficient antecedent basis. Accordingly, Applicant respectfully requests the Examiner to withdraw the rejections of claims 8 and 9 under 35 U.S.C. §112, second paragraph.

II. REJECTIONS UNDER 35 U.S.C. §102(b):

The Examiner has rejected claims 1-81 under 35 U.S.C. §102(b) as being anticipated by the IBM Technical Disclosure Bulletin Vol. 32, No. 8A January 1990 (hereinafter "Bulletin"). Applicant respectfully traverses these rejections for at least the reasons stated below and respectfully requests that the Examiner reconsider and withdraw these rejections.

For a claim to be anticipated under 35 U.S.C. §102, each and every claim limitation must be found within the cited prior art reference and arranged as required by the claim. M.P.E.P. §2131.

Applicant respectfully asserts that the Bulletin does not disclose "providing an application framework, wherein said application framework logs on a user with a first level of access in said underlying operating system" as recited in claim 1 and similarly in claims 28 and 55. The Examiner cites page 304 of the Bulletin as disclosing the above-cited claim limitation. Paper No. 6, page 3. Applicant respectfully traverses and asserts that the Bulletin instead discloses that user management services will check the profile of the specified user and verify that the password provided is that of the named user. Page 304. The Bulletin further discloses that if the password is correct for the user, the user is marked as logged on and may subsequently access authorize system objects. Page 304. There is no language in the Bulletin of providing an application framework. Neither is there any language in the Bulletin of providing an application framework where the application framework logs on a user with a first level of access. Neither is there any language in the Bulletin of providing an application framework where the application framework logs on a user with a first level of access in the underlying operating system. The Examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the user management services of the Bulletin provides an application framework where the application framework logs on a user with a first level of access in the underlying operating system. *Ex parte Levy*, 17 U.S.P.Q.2d 1461, 1464 (Bd. Pat. App. & Inter. 1990). That is, the Examiner must provide extrinsic evidence that must make clear that the user management services of the Bulletin provides an application framework where the application framework logs on a user with a first level of access in the underlying operating system, and that it would be so recognized by persons of ordinary skill. *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999). Thus, the Bulletin does not disclose all of the limitations of claims 1, 28 and 55, and thus the Bulletin does not anticipate claims 1, 28 and 55. M.P.E.P. §2131.

Applicant further asserts that the Bulletin does not disclose "generating an application framework sign-on screen" as recited in claim 1 and similarly in claims 28 and 55. The Examiner cites pages 303-304 of the Bulletin as disclosing the above-cited claim limitation. Paper No. 6, page 3. Applicant respectfully traverses. As stated above, the Bulletin instead discloses that user management services will check the profile of the specified user and verify that the password provided is that of the named user. Page 304. The Bulletin further discloses that if the password is correct for the user, the user is marked as logged on and may subsequently access authorize system objects. Page 304. As stated above, there is no language in the cited passage that discloses an application framework. Neither is there any language in the cited passage that discloses an application framework sign-on screen. The Examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the Bulletin discloses generating an application framework sign-on screen. *Ex parte Levy*, 17 U.S.P.Q.2d 1461, 1464 (Bd. Pat. App. & Inter. 1990). That is, the Examiner must provide extrinsic evidence that must make clear that the Bulletin discloses generating an application framework sign-on screen, and that it would be so recognized by persons of ordinary skill. *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999). Thus, the Bulletin does not disclose all of the limitations of claims 1, 28 and 55, and thus the Bulletin does not anticipate claims 1, 28 and 55. M.P.E.P. §2131.

Applicant further asserts that the Bulletin does not disclose "entering a logon input on said generated application framework sign-on screen" as recited in claim 1 and similarly in claims 28 and 55. The Examiner cites pages 303-304 of the Bulletin as disclosing the above-cited claim limitation. Paper No. 6, page 3. Applicant respectfully traverses. As stated above, the Bulletin instead discloses that user management services will check the profile of the specified user and verify that the password provided is that of the named user. Page 304. The Bulletin further discloses that if the password is correct for the user, the user is marked as logged on and may subsequently access authorize system objects. Page 304. As stated above, there is no language in the cited passage that discloses an application framework. Neither is there any language in the cited passage that discloses an application framework sign-on screen. Neither is there any language in the cited passage that discloses entering a login input on the generated application framework sign-on screen. The Examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the Bulletin discloses entering a logon input on the generated application framework sign-on screen. *Ex parte Levy*, 17 U.S.P.Q.2d 1461, 1464 (Bd. Pat. App. & Inter. 1990). That is, the Examiner must provide extrinsic evidence that must make clear that the Bulletin discloses entering a logon input on the generated application framework sign-on screen, and that it would be so recognized by persons of ordinary skill. *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999). Thus, the Bulletin does not disclose all of the limitations of claims 1, 28 and 55, and thus the Bulletin does not anticipate claims 1, 28 and 55. M.P.E.P. §2131.

Applicant further asserts that the Bulletin does not disclose "comparing said logon input with an application framework security database to determine level of access" as recited in claim 1 and similarly in claims 28 and 55. The Examiner cites page 304 of the Bulletin as disclosing the above-cited claim limitation. Paper No. 6, page 3. Applicant respectfully traverses. As stated above, the Bulletin instead discloses that user management services will check the profile of the specified user and verify that the password provided is that of the named user. Page 304. The Bulletin further discloses that if the password is correct for the user, the user is marked as logged on and may subsequently access authorize system objects. Page 304. As stated above, there is no language in the cited passage that discloses an application framework. Neither is there any language in the cited passage that discloses comparing logon input with an application framework security database to determine the level of access. Thus, the Bulletin does not disclose all of the limitations of claims 1, 28 and 55, and thus the Bulletin does not anticipate claims 1, 28 and 55. M.P.E.P. §2131.

Claims 2-27, 29-54 and 56-81 each recite combinations of features including the above combinations, and thus are not anticipated for at least the above-stated reasons. Claims 2-27, 29-54 and 56-81 recite additional features, which, in combination with the features of the claims upon which they depend are not anticipated by the Bulletin.

For example, the Bulletin does not disclose "selecting an indication of said first level of access" as recited in claim 2 and similarly in claims 29 and 56. Further, the Bulletin does not disclose "selecting an indication of a second level of access" as recited in claim 15 and similarly in claims 42 and 69. The Examiner cites page 304 of the Bulletin as disclosing the above-cited claim limitations. Paper No. 6, page 3. Applicant respectfully traverses. As stated above, the Bulletin instead discloses that user management services will check the profile of the specified user and verify that the password provided is that of the named user. Page 304. The Bulletin further discloses that if the password is correct for the user, the user is marked as logged on and may subsequently access authorize system objects. Page 304. There is no language in the cited passage that discloses selecting an indication of a first level of access. Similarly, there is no language in the cited passage that discloses selecting an indication of a second level of access. There is no indication to be selected where the indication corresponds to either a first or a second level of access. Thus, the Bulletin does not disclose all of the limitations of claims 2, 15, 29, 42, 56 and 69, and thus the Bulletin does not anticipate claims 2, 15, 29, 42, 56 and 69. M.P.E.P. §2131.

Applicant further asserts that the Bulletin does not disclose "wherein said user is logged onto said underlying operating system and an application environment with said first level of access thereby bypassing said initial sign-on screen of said underlying operating system with said single sign-on" as recited in claim 3 and similarly in claims 30 and 57. The Examiner has not cited any passage in the Bulletin as specifically disclosing the above-cited claim limitation. The Examiner merely states that claims 3, 30 and 57 are rejected by the Bulletin but does not cite a passage in the Bulletin that allegedly discloses each element in the above-cited claim limitation. In order to establish a *prima facie* case of anticipation, the Examiner must provide a reference that expressly or inherently describes every element as set forth in the claim. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987); M.P.E.P. §2131. Since the Examiner has not provided any evidence that the Bulletin expressly or inherently describes the above-cited claim limitation, the Examiner has not presented a *prima facie* case of anticipation in rejecting claims 3, 30 and 57. M.P.E.P. §2131.

Applicant further asserts that the Bulletin does not disclose "wherein if said logon input is not entitled to a second level of access according to said application framework security database, then said user is logged onto an application environment and said underlying operating system as said first level of access" as recited in claim 4 and similarly in claims 31 and 58. Applicant further asserts that the Bulletin does not disclose "wherein if said logon input is not entitled to a second level of access according to said application framework security database, then an indication of said second level of access will not be generated to said user, wherein said user is restricted to said first level of access" as recited in claim 10 and similarly in claims 37 and 64. Applicant further asserts that the Bulletin does not disclose "wherein if said logon input is not entitled to said second level of access according to said application framework security database, then said user is restricted to said first level of access" as recited in claim 16 and similarly in claims 43 and 70. The Examiner cites pages 303-304 of the Bulletin as disclosing the above-cited claim limitations. Paper No. 6, page 4. Applicant respectfully traverses.

The Bulletin instead discloses that user management services will check the profile of the specified user and verify that the password provided is that of the named user. Page 304. The Bulletin further discloses that if the password is correct for the user, the user is marked as logged on and may subsequently access authorize system objects. Page 304. There is no language in the cited passage that discloses logging a user onto an application environment and the underlying operating system as a first level of access. Neither does this language disclose logging a user onto an application environment and an underlying operating system as a first level of access if the logon input is not entitled to a second level of access according to an application framework security database. Neither does this language disclose not generating an indication of a second level of access. Neither does this language disclose not generating an indication of a second level of access if the logon input is not entitled to a second level of access according to an application framework security database. Neither does this language disclose that the user is restricted to a first level of access. Neither does this language disclose that the user is restricted to a first level of access if the login input is not entitled to a second level of access according to an application framework security database. Thus, the Bulletin does not disclose all of the limitations of claims 4, 10, 16, 31, 37, 43, 58, 64 and 70, and thus the Bulletin does not anticipate claims 4, 10, 16, 31, 37, 43, 58, 64 and 70. M.P.E.P. §2131.

Applicant further asserts that the Bulletin does not disclose "executing a switch user program to switch said user to said second level of access" as recited in claim 6 and similarly in claims 34 and 61. Applicant further asserts that the Bulletin does not disclose "generating an indication of said second level of access" as recited in claim 11 and similarly in claims 38 and 65. Applicant further asserts that the Bulletin does not disclose "executing a switch user program to switch level of access to said second level of access by selecting said indication of said second level of access" as recited in claim 12 and similarly in claims 39 and 66. Applicant further asserts that the Bulletin does not disclose "executing a switch user program to switch said user to said second level of access" as recited in claim 17 and similarly in claims 44 and 71. The Examiner cites page 303 of the Bulletin as disclosing the above-cited claim limitations. Paper No. 6, page 4. Applicant respectfully traverses.

The Bulletin instead discloses that users may have different levels of authority which will allow them to perform different levels of function or access different sets of objects. Page 303. The Bulletin further discloses that a subsystem may query user management systems to determine a user's authority to help it determine what resources may be made available to the user. Page 303.

None of this language discloses executing a program to switch the user to a second level of access. Neither does this language disclose generating an indication of a second level of access. Neither does this language disclose executing a program to switch the level of access to a second level of access. Neither does this language disclose executing a program to switch the level of access to a second level of access by selecting an indication of a second level of access. Neither does this language disclose executing a program to switch the user to a second level of access. Thus, the Bulletin does not disclose all of the limitations of claims 6, 11, 12, 17, 34, 38, 39, 44, 61, 65, 66 and 71, and thus the Bulletin does not anticipate claims 6, 11, 12, 17, 34, 38, 39, 44, 61, 65, 66 and 71. M.P.E.P. §2131.

Applicant further asserts that the Bulletin does not disclose "wherein said application framework security database shows system operator information, wherein said application framework security database defines at least one of the following: users, passwords, groups of users and application specific authorizations" as recited in claim 7 and similarly in claims 33 and 60. As understood by the Applicant, the Examiner cites page 304 of the Bulletin as disclosing the above-cited claim limitation. Paper No. 6, page 3. Applicant respectfully traverses.

As stated above, the Bulletin instead discloses that user management services will check the profile of the specified user and verify that the password provided is that of the named user. Page 304. The Bulletin further discloses that if the password is correct for the user, the user is marked as logged on and may subsequently access authorize system objects. Page 304. There is no language in the cited passage that discloses an application framework security database that shows system operator information. Neither is there any language in the cited passage that discloses an application framework security database that defines at least one of the following: users, passwords, groups of users and application specific authorizations. Thus, the Bulletin does not disclose all of the limitations of claims 7, 33 and 60, and thus the Bulletin does not anticipate claims 7, 33 and 60. M.P.E.P. §2131.

Applicant further asserts that the Bulletin does not disclose "wherein said switch user program switches said user to said second level of access by modifying an underlying operating system's registry" as recited in claim 8 and similarly in claims 13, 35, 40, 62 and 67. The Examiner cites pages 304-305 of the Bulletin as disclosing the above-cited claim limitation. Paper No. 6, page 4. Applicant respectfully traverses and asserts that the Bulletin instead discloses that a remote authorization table is built containing an entry composed of the user's identity, his password and the identity of the node to which the user is logging on. Page 304. The Bulletin further discloses that if the resource to be accessed is on a remote server node, the database manager is called by the subsystem requestor to obtain the userid/password for the target server node to pass to it. Page 304. The Bulletin further discloses that if no userid/password is in the remote authorization table for the requested node, the most recently used remote userid/password for another node is returned. Page 304. The Bulletin further discloses that if no remote logon has occurred, then the local userid/password is returned to the sub-system requestor for use on the assumption that the user's userid/password may be the same on the remote server as the most recently used id. Pages 304-305. The Bulletin further discloses if the information returned is other than that of the requested node, a remote authorization table entry is built, composed of the user-supplied node name and the userid and password that were returned. Page 305.

This language is not the same as switching a user to a second level of access. The Bulletin does not disclose switching a user to a different level of access. Neither is there any language in the cited passage that discloses switching a user to a second level of access by modifying an underlying operating system's registry. Thus, the Bulletin does not disclose all of the limitations of claims 8, 13, 35, 40, 62 and 67, and thus the Bulletin does not anticipate claims 8, 13, 35, 40, 62 and 67. M.P.E.P. §2131.

Applicant further asserts that the Bulletin does not disclose "wherein said switch user program logs off said user with said first level of access, wherein said underlying operating system logs on said user with said second level of access" as recited in claim 9 and similarly in claims 14, 36, 41, 63 and 68. The Examiner cites pages 303-304 of the Bulletin as disclosing the above-cited claim limitation. Paper No. 6, page 4. Applicant respectfully traverses.

As stated above, the Bulletin instead discloses that users may have different levels of authority which will allow them to perform different levels of function or access different sets of objects. Page 303. The Bulletin further discloses that a subsystem may query user management systems to determine a user's authority to help it determine what resources may be made available to the user. Page 303. The Bulletin further discloses that the user management services will check the profile of the specified user and verify that the password provided is that of the named user. Page 304. The Bulletin further discloses that if the password is correct for the user, the user is marked as logged on and may subsequently access authorize system objects. Page 304. The Bulletin further discloses that when completed, the user issues a logoff command and must subsequently logon again to access protected system objects. Page 304.

None of this language discloses logging on a user with a second level of access by an underlying operating system. Neither does this language disclose logging off a user with a first level of access by a program. Instead, the Bulletin discloses that the user issues a logoff command. Thus, the Bulletin does not disclose all of the limitations of claims 9, 14, 36, 41, 63 and 68, and thus the Bulletin does not anticipate claims 9, 14, 36, 41, 63 and 68. M.P.E.P. §2131.

Applicant further asserts that the Bulletin does not disclose "transferring said logon input to said underlying operating system for verification" as recited in claim 18 and similarly in claims 45 and 72. The Examiner cites page 303 of the Bulletin as disclosing the above-cited claim limitation. Paper No. 6, page 4. Applicant respectfully traverses.

As stated above, the Bulletin instead discloses that users may have different levels of authority which will allow them to perform different levels of function or access different sets of objects. Page 303. The Bulletin further discloses that a subsystem may query user management systems to determine a user's authority to help it determine what resources may be made available to the user. Page 303. There is no language in the cited passage that discloses transferring the logon input to an underlying operating for verification. Thus, the Bulletin does not disclose all of the limitations of claims 18, 45 and 72, and thus the Bulletin does not anticipate claims 18, 45 and 72. M.P.E.P. §2131.

Applicant further asserts that the Bulletin does not disclose "comparing said logon input with an underlying operating system security database, wherein if said underlying operating system security database verifies said user with access to said second level of access, then said switch user program switches said user to said second level of access" as recited in claim 19 and similarly in claims 46 and 73. The Examiner cites page 303 of the Bulletin as disclosing the above-cited claim limitation. Paper No. 6, page 4. Applicant respectfully traverses. As stated above, the Bulletin instead discloses that users may have different levels of authority which will allow them to perform different levels of function or access different sets of objects. Page 303. The Bulletin further discloses that a subsystem may query user management systems to determine a user's authority to help it determine what resources may be made available to the user. Page 303. There is no language in the cited passage that discloses switching the user to a second level of access. Neither is there any language in the cited passage that discloses switching the user to a second level of access if the user has access to the second level of access. Thus, the Bulletin does not disclose all of the limitations of claims 19, 46 and 73, and thus the Bulletin does not anticipate claims 19, 46 and 73. M.P.E.P. §2131.

Applicant further asserts that the Bulletin does not disclose "wherein said switch user program switches said user to said second level of access by modifying an underlying operating system's registry" as recited in claim 20 and similarly in claims 47 and 74. The Examiner cites pages 304-305 of the Bulletin as disclosing the above-cited claim limitation. Paper No. 6, page 4. Applicant respectfully traverses. As stated above, the Bulletin instead discloses a remote authorization table is built containing an entry composed of the user's identity, his password and the identity of the node to which the user is logging on. Page 304. The Bulletin further discloses that if the resource to be accessed is on a remote server node, the database manager is called by the subsystem requestor to obtain the userid/password for the target server node to pass to it. Page 304. The Bulletin further discloses that if no userid/password is in the remote authorization table for the requested node, the most recently used remote userid/password for another node is returned. Page 304. The Bulletin further discloses that if no remote logon has occurred, then the local userid/password is returned to the sub-system requestor for use on the assumption that the user's userid/password may be the same on the remote server as the most recently used id. Pages 304-305. The Bulletin further discloses if the information returned is other than that of the requested node, a remote authorization table entry is built, composed of the user-supplied node name and the userid and password that were returned. Page 305.

There is no language in the cited passage that discloses switching the user to a second level of access. Neither is there any language in the cited passage that discloses switching the user to a second level of access by modifying an underlying operating system's registry. Thus, the Bulletin does not disclose all of the limitations of claims 20, 47 and 74, and thus the Bulletin does not anticipate claims 20, 47 and 74. M.P.E.P. §2131.

Applicant further asserts that the Bulletin does not disclose "wherein said switch user program logs off said user with said first level of access, wherein said underlying operating system logs on said user with said second level of access" as recited in claim 21 and similarly in claims 48 and 75. The Examiner cites page 304 as disclosing the above-cited claim limitation. Paper No. 6, page 4. Applicant respectfully traverses. As stated above, the Bulletin discloses that the user management services will check the profile of the specified user and verify that the password provided is that of the named user. Page 304. The Bulletin further discloses that if the password is correct for the user, the user is marked as logged on and may subsequently access authorize system objects. Page 304. The Bulletin further discloses that when completed, the user issues a logoff command and must subsequently logon again to access protected system objects. Page 304.

There is no language in the cited passage that discloses logging off a user with a first level of access by a program. Instead, the Bulletin discloses that the user issues a logoff command. Neither is there any language in the cited passage that discloses logging on the user with a second level of access by an underlying operating system. Thus, the Bulletin does not disclose all of the limitations of claims 21, 48 and 75, and thus the Bulletin does not anticipate claims 21, 48 and 75. M.P.E.P. §2131.

Applicant further asserts that the Bulletin does not disclose "comparing said logon input with an underlying operating system security database, wherein if said underlying operating system security database does not verify said user with access to said second level of access, then the method further comprises the step of: requesting from said user a logon identification; and comparing said logon identification with said underlying operating system security database" as recited in claim 22 and similarly in claims 49 and 76. The Examiner cites page 303 of the Bulletin as disclosing the above-cited claim limitations. Paper No. 6, page 4. Applicant respectfully traverses.

As stated above, the Bulletin instead discloses that users may have different levels of authority which will allow them to perform different levels of function or access different sets of objects. Page 303. The Bulletin further discloses that a subsystem may query user management systems to determine a user's authority to help it determine what resources may be made available to the user. Page 303.

There is no language in the cited passage that discloses not verifying the user with access to a second level of access. Neither is there any language in the cited passage that discloses that the user is requested for logon identification, which is compared with a security database, if the user is not verified with access to a second level of access. Thus, the Bulletin does not disclose all of the limitations of claims 22, 49 and 76, and thus the Bulletin does not anticipate claims 22, 49 and 76. M.P.E.P. §2131.

Applicant further asserts that the Bulletin does not disclose "wherein if said underlying operating system security database verifies said user with access to said second level of access, then said switch user program switches said user to said second level of access" as recited in claim 25 and similarly in claims 52 and 79. The

Examiner cites page 303 of the Bulletin as disclosing the above-cited claim limitation. Paper No. 6, page 4. Applicant respectfully traverses.

As stated above, the Bulletin instead discloses that users may have different levels of authority which will allow them to perform different levels of function or access different sets of objects. Page 303. The Bulletin further discloses that a subsystem may query user management systems to determine a user's authority to help it determine what resources may be made available to the user. Page 303.

There is no language in the cited passage that discloses switching a user to a second level of access. Neither does this language disclose switching a user to a second level of access if the underlying operating system security database verifies the user with access to the second level of access. Thus, the Bulletin does not disclose all of the limitations of claims 25, 52 and 79, and thus the Bulletin does not anticipate claims 25, 52 and 79. M.P.E.P. §2131.

Applicant further asserts that the Bulletin does not disclose "wherein said switch user program switches said user to said second level of access by modifying an underlying operating system's registry" as recited in claim 26 and similarly in claims 53 and 80. The Examiner cites pages 304-305 of the Bulletin as disclosing the above-cited claim limitation. Paper No. 6, page 4. Applicant respectfully traverses.

As stated above, the Bulletin instead discloses a remote authorization table is built containing an entry composed of the user's identity, his password and the identity of the node to which the user is logging on. Page 304. The Bulletin further discloses that if the resource to be accessed is on a remote server node, the database manager is called by the subsystem requestor to obtain the userid/password for the target server node to pass to it. Page 304. The Bulletin further discloses that if no userid/password is in the remote authorization table for the requested node, the most recently used remote userid/password for another node is returned. Page 304. The Bulletin further discloses that if no remote logon has occurred, then the local userid/password is returned to the sub-system requestor for use on the assumption that the user's userid/password may be the same on the remote server as the most recently used id. Pages 304-305. The Bulletin further discloses if the information returned is other than that of the requested node, a remote authorization table entry is built, composed of the user-supplied node name and the userid and password that were returned. Page 305.

This language does not disclose switching the user to a second level of access. Neither does this language disclose switching the user to a second level of access by a program. Neither does this language disclose switching the user to a second level of access by a program by modifying an underlying operating system's registry. Thus, the Bulletin does not disclose all of the limitations of claims 26, 53 and 80, and thus the Bulletin does not anticipate claims 26, 53 and 80. M.P.E.P. §2131.

Applicant further asserts that the Bulletin does not disclose "wherein said switch user program logs off said user with said first level of access, wherein said underlying operating system logs on said user with said second level of access" as recited in claim 27 and similarly in claims 54 and 81. Based on Applicant's understanding of the Office Action, the Examiner cites pages 303-304 of the Bulletin as disclosing the above-cited claim limitation. Paper No. 6, page 3. Applicant respectfully traverses.

As stated above, the Bulletin instead discloses that user management services will check the profile of the specified user and verify that the password provided is that of the named user. Page 304. The Bulletin further discloses that if the password is correct for the user, the user is marked as logged on and may subsequently access authorize system objects. Page 304. There is no language in the cited passage that discloses a program logging off a user with a first level of access. Neither is there any language in the cited passage that discloses an underlying operating system logging on the user with a second level of access. Thus, the Bulletin does not disclose all of the limitations of claims 27, 54 and 81, and thus the Bulletin does not anticipate claims 27, 54 and 81. M.P.E.P. §2131.

Applicant further asserts that the Bulletin does not disclose "wherein if said underlying operating system security database does not verify said user with access to said second level of access, then said user is restricted to said first level of access" as recited in claim 24 and similarly in claims 51 and 78. The Examiner cites pages 303-304 of the Bulletin as disclosing the above-cited claim limitations. Paper No. 6, page 5. Applicant respectfully traverses.

As stated above, the Bulletin instead discloses that users may have different levels of authority which will allow them to perform different levels of function or access different sets of objects. Page 303. The Bulletin further discloses that a subsystem may query user management systems to determine a user's authority to help it determine what resources may be made available to the user. Page 303. The Bulletin further discloses that the user management services will check the profile of the specified user and verify that the password provided is that of the named user. Page 304. The Bulletin further discloses that if the password is correct for the user, the user is marked as logged on and may subsequently access authorize system objects. Page 304. The Bulletin further discloses that when completed, the user issues a logoff command and must subsequently logon again to access protected system objects. Page 304.

There is no language in the cited passage that discloses restricting the user to a first level of access. Neither is there any language in the cited passage that discloses restricting the user to a first level of access if the underlying operating system security database does not verify the user with access to the second level of access. Thus, the Bulletin does not disclose all of the limitations of claims 27, 54 and 81, and thus the Bulletin does not anticipate claims 24, 51 and 78. M.P.E.P. §2131.

As a result of the foregoing, Applicant respectfully asserts that not each and every claim limitation was found within the cited prior art reference, and thus claims 1-81 are not anticipated by the Bulletin. M.P.E.P. §2131.

III. CONCLUSION:

As a result of the foregoing, it is asserted by Applicant that claims 1-81 in the Application are in condition for allowance, and Applicant respectfully requests an allowance of such claims. Applicant respectfully requests that the Examiner call Applicant's attorney at the below listed number if the Examiner believes that such a discussion would be helpful in resolving any remaining issues.

Respectfully submitted,

WINSTEAD SECHREST & MINICK P.C.

Attorneys for Applicant

By:____________________
Robert A. Voigt, Jr.
Reg. No. 47,159
Kelly K. Kordzik
Reg. No. 36,571

P.O. Box 50784
Dallas, TX 75201
(512) 370-2832